This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-6 (cancelled).

7 (currently amended). A method of communicating with a first computing device, said method comprising the acts of:

encrypting information destined for said first computing device;

creating an HTTP request which includes an address of said first device and the encrypted information; and

transmitting a web page comprising said HTTP request to a second computing device different from said first computing device,

wherein said second computing device is associated with a purchaser of content, wherein said first computing device provides said content, and wherein the encrypted information includes ~~information relating to the purchase of said content, wherein the encrypted information includes information which identifies said purchaser~~ a public portion of a key pair associated with said purchaser, said key pair having been issued to said purchaser for use on said second computing device upon condition of said purchaser tendering authenticatable credentials and upon further condition of said key pair not having been previously been issued for use by said purchaser on a number of devices that exceeds a limit.

8-10 (cancelled).

11 (previously presented). A computer readable medium having computer-executable instructions to perform the method of claim 7.

12-13 (cancelled).

14 (currently amended). A method of communicating with a first computing device through a second computing device, said method comprising the acts of:

encrypting information such that the encrypted information is decryptable by a secret;

transmitting the encrypted information to said second computing device, said encrypted information being transmittable to said first computing device upon instruction from a user operating said second computing device, wherein said secret is not accessible to either said second computing device or said user; and

sharing said secret, wherein the encrypted information ~~includes information relating to the purchaser of said content~~ comprises a public portion of a key pair associated with a user of said second computing device, said key pair having been issued to said user and bound to said second computing device, a private portion of said key pair being usable only on devices to which said key pair is bound, said key pair having been bound to said second computing device on condition of said key pair not having previously been bound to a number of devices that exceeds a pre-defined or determinable limit.

15-20 (cancelled).

21 (currently amended). A method of communicating with a first computing device through a second computing device, said method comprising the acts of:

encrypting information such that the encrypted information is decryptable by a secret;

transmitting the encrypted information to said second computing device, said encrypted information being transmittable to said first computing device upon instruction from a user operating said second computing device, wherein said secret is not accessible to either said second computing device or said user, and wherein said encrypted information comprises a public portion of a key pair associated with said user, said key pair being bound to said second computing device, a private portion of said key pair not being usable on devices to which said key pair has not been bound, said key pair having been bound to said second device after satisfying a condition that said key pair has not previously been bound to a number of devices that exceeds a limit, and after satisfying a further condition that said user provide authenticatable credentials to an entity that binds said key pair to said second device; and

sharing said secret by performing either of the following acts:

providing said secret to said first computing device or to a party associated with said first computing device; or

receiving said secret from said first computing device or from a party associated with said first computing device,

wherein said secret comprises a symmetric key, and wherein said encrypting act comprises encrypting said information with said symmetric key.

22 (previously presented). The method of claim 21, further comprising the act of including a timestamp in the encrypted information.

23 (cancelled).

24 (currently amended). A method of facilitating electronic content distribution comprising the acts of:

providing, to a first party for use on a first computing device, a first set of computer-executable instructions which encrypts information based on a unique id that maps into a shared secret, the encrypted information being includable in an HTTP request which includes a network address of a second computing device; and

providing, to a second party for use on said second computing device, a second set of computer-executable instructions which decrypts the encrypted information, said encrypted information comprising a public portion of a key pair, said key pair being associated with a third party who is distinct from both said first party and said second party, said key pair having been issued to said third party and bound to a third computing device that is distinct from both said first computing device and said second computing device, a private portion of said key pair being usable only on devices to which said key pair is bound, said key pair having been bound to said third computing device on condition of the number of devices to which said key pair has been previously bound not exceeding a limit.

25 (original). The method of claim 24, wherein said first party comprises a seller of electronic content, wherein said second party comprises a provider of electronic content sold by said first party, and wherein said encrypted information relates to a transaction between said first party and a consumer of electronic content.

26 (original). The method of claim 24, wherein said HTTP request comprises a POST request, and wherein said encrypted information is included in the body of said POST request.

27 (original). The method of claim 24, wherein said HTTP request comprises a GET request, and wherein said encrypted information is appended to said GET request as a parameter.

28 (original). The method of claim 24, wherein said first set of computer-executable instructions comprises a COM object.

29 (original). The method of claim 28, wherein said first set of computer-executable instructions exposes an ENCRYPT method for use by a third set of computer-executable instruction which runs on said first computing device.

30 (original). The method of claim 24, wherein a secret symmetric key is accessible to or known by each of said first computing device and said second computing device, and wherein said first set of computer-executable instructions uses said secret symmetric key to encrypt said information.

31 (original). The method of claim 24, wherein said information includes information identifying an item of content which said second computing device provides.

32 (original). The method of claim 24, wherein said information includes information identifying a purchaser of an item of content.

33 (currently amended). A method of building a client-server request, said method comprising the acts of:

encrypting first information so as to be decryptable by a secret accessible to a first server;

including an address associated with said first server in said client-server request; ~~and~~

including the encrypted information in said client-server request; and

transmitting said client-server request to a client on which said client-server request is executable to contact said first server and to transmit said encrypted information to said first server, wherein the encrypted information comprises a public portion of a key pair bound to said client, said key pair being bindable to a number of devices not in excess of a pre-defined or determinable limit, a private portion of said public key not being usable on devices to which said key pair is not bound, said key pair having been bound to said client upon determination that binding said key pair to said client would not cause the number of devices to which said key pair is bound to exceed said limit.

34 (original). The method of claim 33, wherein the encrypted information includes information relating to a transaction to purchase a content item, wherein said first server furthers at least some aspect of said transaction.

35 (original). The method of claim 34, wherein the encrypted information includes information which identifies a purchaser of said content item.

36 (original). The method of claim 34, wherein the encrypted information includes information which identifies said content item.

37 (original). The method of claim 34, wherein the encrypted information includes a timestamp.

38 (original). The method of claim 34, wherein said first server provides said content item.

39 (original). The method of claim 33, wherein said secret comprises a symmetric key, and wherein the encrypted information is generated by encrypting cleartext information with said symmetric key.

40 (original). The method of claim 33, wherein said client-server request comprises an HTTP request.

41 (original). The method of claim 40, wherein said HTTP request comprises a POST request, and wherein the encrypted information is included in the body of said POST request.

42 (original). The method of claim 40, wherein said HTTP request comprises a GET request, and wherein the encrypted information is appended to said GET request as a parameter.

43 (original). A computer-readable medium having computer-executable instructions to perform the method of claim 33.

44 (currently amended). A method of distributing electronic content, said method comprising the acts of:

receiving, at a first computing device from a second computing device, an order for a content item; and

providing, from said first computing device to said second computing device, data comprising:

a network address of a third computing device; and

encrypted information that comprises a public portion of a key pair associated with an entity that placed said order, said key pair being bound to one or more devices including said second computing device, said key pair being bindable to a number of devices not in excess of a limit, said key pair having been bound to said second computing device conditioned upon a determination that binding said key pair to said second computing device would not cause the number of devices to which said key pair is bound to exceed said limit;

wherein said third computing device processes said order by using at least some of said encrypted information.

45 (original). The method of claim 44, wherein said data comprises an HTTP POST request, and wherein said encrypted information is included in the body of said POST request.

46 (original). The method of claim 44, wherein said data comprises an HTTP GET request.

47 (original). The method claim 44, wherein said encrypted information includes information identifying said content item.

48 (original). The method of claim 44, wherein said encrypted information includes information identifying the individual who issued said order for said content item.

49 (original). The method of claim 44, wherein said encrypted information includes a timestamp.

50 (original). The method of claim 44, wherein said data further comprises a hash of said encrypted information, said hash being computed prior to encryption of said information.

51 (original). The method of claim 50, wherein said hash is computed using an SHA1 algorithm.

52 (original). The method of claim 44, wherein said content item does not reside on said first computing device.

53 (original). A computer-readable medium having computer-executable instructions to perform the method of claim 44.

54 (currently amended). A computer-readable medium having computer-executable instructions for performing steps comprising:

receiving parameters that identify characteristics of a first transaction between a first client and a first server, said first transaction being a purchase transaction;

encrypting one or more of said parameters, said one or more parameters including a public portion of a key pair bound to said first client, said key pair being bindable to a number of clients not in excess of a limit, a private portion of said key pair not being usable on clients to which said key pair is not bound, said key pair having been bound to said first client upon condition that binding said key pair to said first client would not cause the number of devices to which said key pair is bound to exceed said limit;

returning said encrypted parameters to said first client in a format such that a second server may receive said encrypted parameters from said first client, validate said first transaction, and initiate a second transaction without any interaction with said first server.

55 (original). The computer-readable medium of claim 54, wherein said computer-executable instructions comprise a COM object.

56 (original). The computer-readable medium of claim 54, wherein said first transaction relates to the sale of electronic content.

57 (original). The computer-readable medium of claim 56, wherein said second transaction comprises downloading said electronic content from said second server to said first client.

58 (original). The computer-readable medium of claim 56, wherein said parameters comprise end-use information that enables the individualization of said electronic content.

59 (original). The computer-readable medium of claim 54, wherein said parameters include one or more of the following: information identifying a party to said first transaction, and information identifying an item purchased in said first transaction.

60 (original). The computer-readable medium of claim 54, wherein said steps further comprise including a timestamp in said encrypted parameters.

61 (original). The computer-readable medium of claim 54, wherein said steps further comprise computing a hash of at least some of said encrypted parameters.

62 (original). The computer-readable medium of claim 61, wherein said hash is computed using an SHA1 algorithm.

63 (original). The computer-readable medium of claim 54, wherein said encrypting act comprises applying a secret symmetric key shared between said first server and said second server.

64 (original). The computer-readable medium of claim 54, wherein said format comprises an HTTP request including an address of said first server.